

Publicación	Revista SIC	Fecha	14/06/2019
Soporte	Prensa Escrita	País	España
Circulación	5000	Página	171
Difusión	4000	Tamaño	586.98 cm² (94.16%)
Audiencia	12 000	V.Publicación	1847 EUR (2092 USD)



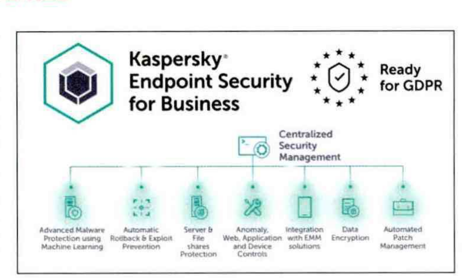
KASPERSKY REFUERZA SU SOLUCIÓN ENDPOINT SECURITY FOR BUSINESS CON CAPACIDADES DE DETECCIÓN AUTOMÁTICA DE ANOMALÍAS EN COMUNICACIONES DE RED

Kaspersky ha introducido varias mejoras en su solución **Kaspersky Endpoint Security for Business** dirigidas a reforzar la protección de los puntos finales y a dotar de mayor seguridad a las comunicaciones de red, especialmente, a las que se conectan a Internet.

Entre sus novedades destaca el nuevo módulo **Adaptive Anomaly Control** que, de forma inteligente, analiza y bloquea aplicaciones y comportamientos anómalos del usuario. Para ello, este componente inteligente analiza el comportamiento de los usuarios y 'recuerda' sus patrones de actividad, permitiéndole bloquear acciones 'fuera de lo normal' para un usuario concreto.

Además, Kaspersky Endpoint Security for Business ofrece ahora una mejor protección contra ciberataques de minería y amenazas en la web. Por ejemplo, para evitar que determinado *malware* se aproveche de los recursos de cálculo de los equipos corporativos, las capacidades de Control Web de la nueva solución incluyen tecnología para desenmascarar y tratar de bloquear en línea las acciones de criptominería. Endpoint Security for Business también incorpora escaneado de tráfico cifrado para la identificación y el bloqueo de aquellas ataques que intenten introducirse en los sistemas sin ser detectados.

Todas estas características vienen respaldadas por técnicas de inteligencia de amenazas, aprendizaje automático, administración de vulnerabilidades y parches de seguridad, así como un conjunto de funcionalidades que ayudan a automatizar las tareas de gestión y control de los dispositivos ligados a la infraestructura corporativa. Además, se pueden integrar con otros productos como Kaspersky Endpoint Detection and Response, y con sistemas SIEM, SOAR –Orquestación y Automatización de la seguridad- y plataformas EDR de terceros a través de la interfaz de programación de aplicaciones, OpenAPI.



Como novedad, también cabe resaltar la disponibilidad de la consola de administración de la solución, Kaspersky Security Center, en su versión web, lo que hace que en el proceso de instalación no se necesite ningún software, ni abrir puertos de red.

Seguridad en *blockchain*

Kaspersky Lab ofrece dos nuevos servicios de protección para entornos *blockchain*. Por un lado, el denominado **Smart Contract Code Review**, diseñado para identificar defectos y características no declaradas, así como discrepancias entre la documentación y la lógica de negocio de los contratos inteligentes. Y, por otro, **Application Security Assessment**, cuya misión es analizar el estado de seguridad de las aplicaciones, ya sean descentralizadas o tradicionales.

Los servicios de seguridad de *blockchain* de Kaspersky incorporan también protección frente al *phishing*, alertando de copias falsas de los intercambios de criptomonedas y de los ICO, así como los servicios Incident Response y Cybersecurity Awareness Training para mejorar el nivel global de 'higiene' en ciberseguridad, de modo que una empresa no caiga víctima de ataques de ingeniería social.

KASPERSKY LAB
www.kaspersky.es

QUALYS EXTIENDE SU PLATAFORMA CLOUD AGENT CON SU NUEVO SERVICIO CLOUD AGENT GATEWAY

Para reforzar su plataforma Cloud Agent, **Qualys** ha presentado su nuevo servicio **Cloud Agent Gateway** (CAG) con el objetivo de simplificar las implementaciones a gran escala, en los entornos de nube híbridos y en local, así como para aumentar la seguridad en sus conexiones de red.

En concreto, el nombre de Cloud Agent Gateway responde a un grupo de dispositivos virtuales administrados desde la plataforma Qualys Cloud para conectar de manera más segura los agentes desplegados en cualquier lugar (incluidos los que están en entornos OT y en redes locales restringidas), a la plataforma Qualys Cloud Platform. Esto permite conectar de una forma más segura el tráfico de Cloud Agent a un dispositivo virtual CAG ubicado dentro de redes locales restringidas o sensibles, extendiendo las implementaciones de los agentes de nube a entornos sensibles como DMZs (redes aisladas del resto de la red interna) y redes industriales con fuerte bloqueo, donde el acceso directo a Internet está restringido. Además, gracias a las capacidades de evaluación y monitorización de Qualys Cloud Platform, las empresas tendrán mayor visibilidad de la seguridad y del cumplimiento de normativas de los activos de TI en estos entornos.

Los nuevos dispositivos CAG también eliminan la barrera de implementación, gestión y mantenimiento de proxis de terceros o pasarelas web seguras para instalaciones de los agentes *cloud* a gran escala, optimizando además el ancho de banda ya sean en grandes entornos o a través de redes más pequeñas, como sucursales.

Al almacenar en caché las actualizaciones, manifiestos y parches para su distribución a los agentes de nube, los clientes pueden evitar el coste y la complejidad de utilizar un Secure Web Gateway comercial, y beneficiarse de "un menor TCO (coste total de propiedad) de las soluciones de seguridad en la nube de Qualys", resalta la compañía.

Qualys Patch Management (PM)

Asimismo, la recién introducida aplicación de gestión de parches, **Qualys PM Cloud**, aprovecha los agentes *cloud* para llevar la administración y remediación de vulnerabilidades de sistemas operativos, como Windows, macOS y Linux, y de más de 300 aplicaciones de terceros, a activos de TI críticos, a través de infraestructuras en local, en nube y *endpoints*.

Con ello Qualys ha creado una plataforma para ayudar a las organizaciones a automatizar todo el ciclo de vida del descubrimiento, priorización y la reparación de vulnerabilidades a escala global. El servicio CAG permite, además, la entrega rápida de los parches de seguridad a los activos de TI críticos mediante su almacenamiento en caché y su distribución local a los componentes de la red.

QUALYS
www.qualys.com